System for the checking of limited access to authorized time slots renewable by means of a portable storage device

Patent number:	DE69507278T
Publication date:	1999-06-10
Inventor:	GIRAULT MARC (FR); REITTER RENAUD (FR); REVILLET MARIE-JOSEPHE (FR)
Applicant:	POSTE (FR)
Classification:	
- international:	G07C9/00; G07F7/08
- european:	A47G29/12M; A47G29/14E; G07C9/00B2; G07C9/00B4; G07F7/08E4; G07F7/10D4; G07F7/10D4E2; G07F7/10D12; G07F7/10E
Application number:	DE19956007278T 19950711
Priority number(s):	FR19940008770 19940713; WO1995FR00935 19950711

Also published as:

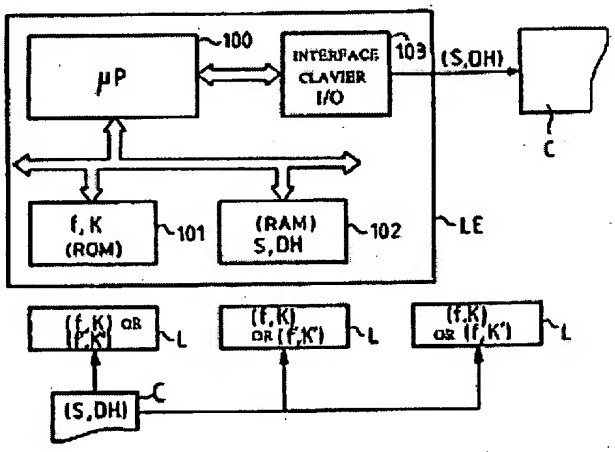
WO9602899 (A1)
EP0719438 (A1)
US5768379 (A1)
FR2722596 (A1)
EP0719438 (B1)

more >>

Report a data error here

Abstract not available for DE69507278T
Abstract of corresponding document: **US5768379**

PCT No. PCT/FR95/00935 Sec. 371 Date Mar. 7, 1996 Sec. 102(e) Date Mar. 7, 1996 PCT Filed Jul. 11, 1995 PCT Pub. No. WO96/02899 PCT Pub. Date Feb. 1, 1996The invention relates to systems for checking access limited to authorized time slots renewable by means of a portable storage device. The system comprises, for this purpose, an element (LE) producing electronic keys formed by a data element pertaining to a time slot and by the signature of this data element. These keys are loaded into devices such as memory cards (C). Electronic locks (L) capable of verifying the signatures are implanted in the different (physical or logical) locations, the access to which has to be guarded. Application to the checking of access to buildings or computer systems.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Übersetzung der europäischen Patentschrift

(87) EP 0 719 438 B1

(10) DE 695 07 278 T2

(51) Int. Cl.[6]: G 07 C 9/00
G 07 F 7/08

(21) Deutsches Aktenzeichen: 695 07 278.1
(86) PCT-Aktenzeichen: PCT/FR95/00935
(86) Europäisches Aktenzeichen: 95 925 045.7
(87) PCT-Veröffentlichungs-Nr.: WO 96/02899
(86) PCT-Anmeldetag: 11. 7. 95
(87) Veröffentlichungstag der PCT-Anmeldung: 1. 2. 96
(87) Erstveröffentlichung durch das EPA: 3. 7. 96
(87) Veröffentlichungstag der Patenterteilung beim EPA: 13. 1. 99
(47) Veröffentlichungstag im Patentblatt: 10. 6. 99

(30) Unionspriorität:
9408770 13. 07. 94 FR

(73) Patentinhaber:
La Poste, Boulogne Billancourt, FR

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, Anwaltssozietät, 80538 München

(84) Benannte Vertragstaaten:
AT, BE, CH, DE, ES, FR, GB, IT, LI, NL, SE

(72) Erfinder:
GIRAULT, Marc, F-14000 Caen, FR; REITTER, Renaud, F-14000 Caen, FR; REVILLET, Marie-Josephe, F-14790 Verson, FR

(54) ZUGANGSKONTROLLSYSTEM MIT AUTORISIERTEN UND MITTELS EINES TRAGBAREN SPEICHERTRÄGERS ERNEUERBAREN STUNDENBEREICHEN

DE 695 07 278 T2

DE 695 07 278 T2

21.01.99

95 925 045.7
LA POSTE

Die Erfindung betrifft ein Zugangskontrollsystem mit autorisierten und mittels eines Speicherträgers erneuerbaren Stundenbereichen.

Die Erfindung betrifft insbesondere das Gebiet der Zugangskontrolle von Gebäuden, Informatiksystemen oder allen Arten von anderen Systemen, deren Benutzung kontrolliert werden muß.

Die bekannteste Art, einen Zugang zu verschließen, besteht darin, ein mechanisches Schloß anzubringen und den Personen mit Zugangsberechtigung einen Schlüssel auszuhändigen, wobei es sich um ein Gebäude oder irgendein anderes Objekt handeln kann. Selbstverständlich beruht der Nachteil dieser Methode auf der Tatsache, daß die mechanischen Schlüssel leicht zu duplizieren sind. Ein solcher Schlüssel kann auch gestohlen und vom Dieb benutzt werden, wobei dann die einzige Abhilfe darin besteht, den Zylinder des Schlosses auszutauschen.

Eine zweite Methode, aber diesmal elektronisch, besteht darin, eine Schloß mit einer Paßwort vorzusehen. Nur die Benutzer, die das Paßwort kennen, können das geschützte Gebäude betreten.

Leider ist diese Lösung nicht sicher. Wenn z.B. ein Benutzer sein Paßwort auf einer Tastur eingibt, ist es ohne weiteres möglich, dieses Paßwort mit einer entsprechenden Elektronik zu lesen, so daß eine Person mit schlechten Absichten es mißbräuchlich benutzen kann.

Außerdem ist bekannt, den Zugang zu Computerprogrammen mittels eines Paßworts zu schützen. Dieser Schutz hat den vorhergehend erwähnten Nachteil.

Man kennt auch ein Authentisierungsverfahren, Kerberos genannt, das ermöglicht, den Zugang zu einem offenen Datennetz zu schützen. Eine Beschreibung dieses Verfahrens findet man in der MIT-Veröffentlichung vom 30. März 1988 mit dem Titel "An Authentification Service for Open Network Systems".

Dieses Verfahren ermöglicht, einen "Kunden", d.h. einen Benutzer zu identifizieren und ihm einen Zugang zu einem Server zu ermöglichen (zu einer Dienstleistung, einer Anwendung, einem Programm), indem es ihm dazu ein elektronisches Ticket und noch

genauer eine mit einem Schlüssel verschlüsselte Information liefert. Dieses Ticket wird durch den Server des "Kunden" erstellt. Andererseits reicht das Ticket nicht aus für eine Zugangserlaubnis und es wird bei diesem Verfahren zusammen mit dem Ticket noch eine zweite verschlüsselte Information benutzt.

Ein solches Verfahren ist schwerfällig und verlangt relativ leistungsstarke Recheneinrichtungen, was kein Hindernis ist bei der vorgesehene Anwendung, aber ein solches werden kann für andere Anwendungen, nämlich solche Anwendungen, bei denen der Speicherplatz und die Recheneinrichtungen nicht so groß sind wie bei einem Server.

Die zweite verschlüsselte Information wird erstellt für einen Zugang zwischen einem Kunden und einem Server und kann nur einmal für diese Verbindung benutzt werden.

Man kann sich außerdem auf das Dokument EP-A-0 122 244 aus dem Stand der Technik beziehen, das der vorliegenden Erfindung am nächsten kommt.

Die vorliegende Erfindung hat die Aufgabe, die oben genannten Nachteile zu beseitigen.

Außerdem ist es erfindungsgemäß nicht nötig, eine schwarze Liste verlorener oder gestohlener oder duplizierter Zugangseinrichtungen zu erstellen und zu verwalten, wie die Folge der Beschreibung zeigt, denn ein verlorener oder gestohlener Träger kann keine Zugangsberechtigung außerhalb des autorisierten Stunden- bzw. Zeitbereichs liefern, wenn diese nicht erneuert wird. Die Aufnahme eines solchen Trägers in eine schwarze Liste ist umso nutzloser, je kürzer die Zugangsberechtigungsdauer ist.

Erfindungsgemäß erfolgt die Zugangskontrolle nicht durch mechanische Einrichtungen sondern durch logische Einrichtungen mittels einer elektronischen Signatur von Daten bezüglich einer vorher festgelegten Zugangsberechtigungsperiode, die die Benutzungsgültigkeit des Trägers begrenzt, in dem sie abgespeichert ist. Erfindungsgemäß wird die Signatur nämlich in dem tragbaren Speicherungsträger abgespeichert, ebenso wie - je nach benutztem Algorithmus -, die Größe um den Zugang zu allen Geräten zu ermöglichen, die das erfindungsgemäße Sicherungssystem enthalten.

21.01.99

Die vorliegende Erfindung hat insbesondere ein Zugangskontrollsystem nach Anspruch 1 zum Gegenstand.

Der Begriff der elektronischen Signatur bzw. Unterschrift muß hier im im weiteren Sinne verstanden werden. Es kann sich um eine elektronische Signatur handeln, die mit Hilfe irgendeines bekannten Verschlüsselungsmechanismus zustande kommt, nämlich Chiffrier- oder Authentisierungsverfahren.

Vorzugsweise umfaßt die die vorher festgelegte Gültigkeitsperiode betreffende Größe DH eine Benutzungsdatums-information und einen Benutzungzeitbereich.

Nach einer Ausführungsart werden meherere Signaturen Sj durch die Schlüsselerstellungseinrichtungen (S) berechnet und aufgezeichnet auf den Trägern der Benutzer, wobei man diese Signaturen aus demselben Geheimschlüssel K und einer Erzeugungs-funktion f wie SJ = f(K, DH, aj) erhält und die Parameter aj dabei vorher festgelegt und in den elektronischen Verriegelungen abgespeichert werden. Man begrenzt nach dieser Ausführungsart die Anzahl der Zugänge eines Benutzers in der betreffenden Periode. Dieser hat ebensoviele Zugangsberechtigungen wie die Anzahl der für die betreffende Periode berechneten und auf seinem Träger abgespeicherten Signaturen. Für jeden Zugang ist eine Signatur erforderlich.

Nach einer Ausführungsart erhält man die Signatur mittels eines Erzeugungsalgorithmus mit geheimem Schlüssel.

Nach einer anderen Ausführungsart kann man die Signatur mittels eines Erzeugungsalgorithmus mit öffentlichem Schlüssel herstellen.

Erfindungsgemäß wird die Signatur in dem Anwendungsfall der öffentlichen Benutzung vorzugsweise mit einem Algorithmus mit öffentlichem Schlüssel hergestellt, d. h. in dem Fall, wo die Überprüfung der Signatur durch Einrichtungen erfolgt, die öffent-lich zugänglich sind.

Nach einer weiteren Ausführungsart ist der zum Erstellen der Signaturen benutzte Schlüssel derselbe für alle Signaturen, die in den Trägern geladen sind und erneuert werden.

Nach einer weiteren Ausführungsart der Erfindung ordnet man diesem Schlüssel K eine Größe Z zu, verschieden je nach

geographischer oder logischer Benutzungszone, um diese Benutzungszonen unterscheiden zu können.

Nach einer weiteren Ausführungsart benutzt man verschiedene Schlüssel, um die periodisch geladenen Signaturen zu erstellen, wobei pro festgelegter geographischer oder logischer Zone ein Schlüssel erstellt wird.

Nach einer anderen Charakteristik der Erfindung kann man einen diversifizierten Schlüssel Kc benutzen, erzeugt mittels einer Diversifikationsfunktion bekannten Typs.

Nach einer weiteren Charakteristik der Erfindung unterteilt man den festgelegten Gültigkeitszeitbereich in eine bestimmte Anzahl von aufeinanderfolgenden Stunden- bzw. Zeitbereichen und erstellt eine Signatur Si für jeden dieser Bereiche.

Die Erfindung wird besser verständlich durch die nachfolgende, erläuternde und nicht einschränkende Beschreibung, bezogen auf die beigefügten Zeichnungen:

- die Figur 1 stellt ein Prinzipschaltbild eines erfindungsgemäßen Systems dar,
- die Figur 2 zeigt das praktische Ausführungsschaltbild der Kontrolleinrichtungen der elektronischen Schlüssel nach der Erfindung,
- die Figur 3 zeigt das praktische Ausführungsschaltbild eines erfindungsgemäßen Speicherungsträgers.

In der Folge der Beschreibung versteht man unter Signier-Entität oder berechtigter Entität die Erstellungseinrichtungen der elektronischen Schlüssel, d.h. der Paare S, DH (elektronische Signaturen und Größen), wobei diese Einrichtungen außerdem das Laden dieser Signaturen in die Speicherungsträger ermöglichen. Man versteht unter elektronischer Verriegelung die Kontrolleinrichtungen der in den Speicherungsträgern gelesenen Größen.

Die Signier-Entität ist erfindungsgemäß fähig, eine elektronische Signatur S mittels einer Erzeugungsfunktion f und eines geheimen Schlüssels K zu erzeugen.

Die elektronische Signatur einer Größe DH durch die Signier-Entität kann S = f (K, DH) geschrieben werden.

Damit die Signatur der Signier-Entität durch jede der den Zugang gewährenden logischen Verriegelungen überprüft werden kann, verfügen diese Verriegelungen über adäquate Verschlüsselungsein-

richtungen. Diese Einrichtungen umfassen einen Prüfalgorithmus f' und einen Prüfschlüssel K', der, je nach dem, ob der Signaturalgorithmus einen geheimen Schlüssel oder einen öffentlichen Schlüssel aufweist, gleich dem geheimen oder öffentlichen Schlüssel der Signier-Entität ist. Im ersten Fall hat man folglich K = K'; im zweiten Fall ist es bei Kenntnis von K' unmöglich, daraus K abzuleiten.

Je nach vorgesehenen Anwendungen befinden sich die elektronischen Verriegelungen in einer öffentlich zugänglichen Umgebung oder in einer abgeschlossenen Umgebung. Wenn die elektronischen Verriegelungen sich in einer öffentlichen Umgebung befinden, benutzt man vorzugsweise einen Algorithmus mit öffentlichem Schlüssel, so daß diese elektronischen Verriegelungen keine geheime Information enthalten und es keinen Grund gibt, ihren Inhalt mit betrügerischer Absicht zu lesen. Derart wird die Sicherheit des Systems erhöht und Vandalismus, da gegenstandslos, vermieden.

Der Speicherungsträger hat dann erfindungsgemäß die Funktion eines elektronischen Schlüssels, der alle elektronischen Verriegelungen öffnen kann, die über ein gesamtes Gebiet oder in einer speziellen Zone eingerichtet sind. Erfindungsgemäß erhält man den elektronischen Schlüssel aus einer eine bestimmte Zugangsberechtigungsperiode betreffenden Größe, die die Gültigkeit des Trägers begrenzt. Diese Periode umfaßt z.B. Datum und Stunde des Beginns des Zeitbereichs und Datum und Stunde des Endes des Zeitbereichs, in der Folge DH genannt. Es kann sich auch um ein Datum und eine Stunde des Endes der Berechtigung handeln. Bei der Zugangskontrolle überprüft die elektronische Verriegelung, die vorteilhafterweise mit einer internen Uhr versehen ist, ob die laufende Datum/Zeit-Information sich innerhalb des Bereichs befindet, und überprüft dann die Signatur mit Hilfe des Prüfschlüssels (geheim oder öffentlich, je nach Fall), über den sie verfügt. Wenn beide Prüfungsbedingungen erfüllt werden, sendet die Verriegelung ein Zugangsberechtigungssignal A.

Wenn z.B. ein Geheimschlüssel-Algorithmus benutzt wird, liest die elektronische Verriegelung den in dem Speicherungsträger aufgezeichneten Bereich DH, liest mittels ihrer internen Uhr die laufende Datums- und Stundeninformation und überprüft, ob diese

Information sich innerhalb des in dem Träger gelesenen Bereichs befindet, und berechnet dann eine Signatur S' = f (K, DH). Die Verriegelung liest ebenfalls die Signatur, die in dem Träger abgespeichert ist und überprüft, ob die berechnete Signatur gleich der gelesenen Signatur ist oder nicht.

Falls man einen Algorithmus mit öffentlichem Schlüssel benutzt, liest die elektronische Verriegelung die den Zeitbereich DH betreffende Größe, liest das Datum und die Stunde ihrer internen Uhr und überprüft, ob dieses Datum und diese Stunde sich auch innerhalb des in dem Träger gelesenen Bereichs befindet. Die elektronische Verriegelung liest ebenfalls die in dem Träger gespeicherte Signatur S und überprüft mit Hilfe der Prüfungsfunktion f' und des K zugeordneten öffentlichen Schlüssels K', ob diese Signatur S wirklich die Signatur der Größe DH ist, was folgendermaßen ausgedrückt werden kann:

f' (K', DH, S) = "OK",

wobei die Information "OK" in der Praxis einem Bit mit 1 oder mit 0 entspricht, je nach gewählter Konvention.

In der Folge werden praktische Ausführungsbeispiele detailliert beschrieben. Zum besseren Verständnis kann man sich auf die Figuren 1 bis 3 beziehen.

Wie schon erwähnt, ermöglicht das erfindungsgemäße System, das Führen von schwarzen Listen und deren Verwaltung bei jeder Zugangsanfrage z.B. zu Gebäuden oder Informatiksystemen oder jeder anderen Art von Objekten, wie dies bei den Techniken der vorhergehenden Technik erforderlich ist, zu vermeiden.

Um dieses Ziel zu erreichen, ersetzt die Erfindung die mit einem mechanischen Schlüssel verbundenen traditionellen mechanischen Zugangseinrichtungen durch eine logische Einrichtung, die auf einer elektronischen Signatur beruht, berechnet durch eine berechtigte Entität, die dazu einen geheimen Schlüssel K erhalten hat.

Die Erfindung besteht daher außerdem darin, in jeden Träger eine elektronische Signatur zu laden. Die durch diese elektronische Signatur signierte Größe umfaßt eine Größe, die eine festgelegte Benutzungsgültigkeitsperiode betrifft. Außerhalb dieser Benutzungsgültigkeitsperiode wird die Signatur nicht mehr erkannt und der Zugang wird folglich nicht freigegeben. Wenn nicht

21.01.99

das Laden einer neuen Signatur stattgefunden hat, wird der Zugang nicht mehr freigegeben.

In Figur 1 ist das Schaltbild eines erfindungsgemäßen Systems dargestellt. Dieses System umfaßt Erzeugungseinrichtungen elektronischer Signaturen LE. In der Praxis können diese Einrichtungen durch einen Leser-Codierer gebildet werden, der einen Mikroprozessor oder einen Mikrocontroller umfaßt, programmiert um einen Erzeugungsalgorithmus f durchzuführen. Es kann sich z.B. um einen Algorithmus mit geheimem Schlüssel oder einen Algorithmus mit bekanntem öffentlichem Schlüssel handeln.

Man kann z.B. als Geheimschlüssel-Algorithmus den Algorithmus DES (Data Encrytion Standard) nennen und als Öffentlicher-Schlüssel-Algorithmus den Algorithmus RSA (Rivest Shamir Adleman).

In der Folge der Beschreibung werden diese Algorithmen durch eine Funktion f dargestellt.

Der Leser/Codierer ermöglicht außerdem, die Signaturen in die Speicherungsträger zu laden. Dazu wählt man einen bekannten und an den gewählten Speicherungsträger angepaßten Leser/Codierer. Beispielsweise kann man auf dem Markt vorhandene Leser/Codierer nehmen, die ermöglichen, eine Magnetkarte oder eine Speicherkarte mit bündig eingelassenem Kontakt zu lesen und zu beschreiben, oder einen Leser/Codierer, angepaßt an das Lesen und Beschreiben eines elektronischen Schlüssels mit bündig eingelassenem Kontakt, oder einen Leser/Codierer, angepaßt an das Lesen und Beschreiben von Karten ohne Kontakt.

Das in Figur 1 dargestellte Beispiel zeigt das elektronische Schaltbild eines Leser/Codierers, der an das Lesen und Beschreiben eines Speicherungsträgers des Typs Speicherkarte angepaßt ist.

Dieser Leser/Codierer-Typ ist bekannt und umfaßt einen Mikroprozessor 100 (oder Mikrocontroller) mit einem zugeordneten Programmspeicher 101 des Typs ROM oder EPROM (elektrisch löschbar) und eventuell einen Arbeitsspeicher 102 des Typs RAM.

Dieser Leser/Codierer LE umfaßt ein Eingang/Ausgang-Interface 103, angepaßt an den Speicherungsträger. Es umfaßt im Falle eines kontaktlosen Schreib-/Leseträgers eine Sende-Empfangsantenne. Er umfaßt Kontakte, die angepaßt sind an die bündig eingelassenen Kontakte wie z.B. diejenigen der Chipkarten

oder der elektronischen Schlüssel. Dieser Leser umfaßt außerdem eine nicht dargestellte Tastatur.

Der nichtflüchtige Speicher 101 des Leser/Codierers LE enthält das Anwendungsprogramm der gewählten Funktion f und ein klassisches Lese- und Schreibprogramm für einen Speicherungsträger. Der Schlüssel K wird ebenfalls in diesem Speicher aufgezeichnet.

Die berechnete Signatur kann dieselbe sein für alle Träger. Wenn die Signatur S die Signatur einer Größe DH ist, bedeutet dies, daß diese Größe DH dieselbe für alle Träger ist.

Die berechneten Signaturen können für jeden Träger verschieden sein.

Die für jeden Träger bestimmten Signaturen S können dann im voraus berechnet werden oder nach und nach. Falls sie im voraus berechnet werden, müssen die jede Anwendung betreffenden Größen DH in einem nichtflüchtigen Speicher des Leser/Codierers aufgezeichnet werden. In diesem Falle wird auch eine Tabelle gespeichert, um für jede Anwendung das Paar: Signatur S-Größe DH, das ihr zugeteilt ist, in Übereinstimmung zu bringen.

In diesem Fall, wenn ein Speicherungsträger durch einen Benutzer in den Leser/Codierer eingeführt wird, gibt der Benutzer seine Identifikationsnummer auf der Tastatur des Leser/Codierers ein und der Leser/Codierer kann dann in der Tabelle die Signatur S und die Größe DH, die dieser Benutzung zugeteilt sind, suchen und sie in den Speicher des Trägers laden.

Selbstverständlich kann man anders vorgehen, ohne daß dies das Prinzip der Erfindung verändert. Die Signaturen können nämlich nach und nach berechnet werden, entsprechend dem Bedarf, d.h. bei jeder Ladungsanfrage in den Speicherungsträger durch einen Benutzer. In diesem Fall ist es nicht notwendig, eine Tabelle abzuspeichern, die die verschiedenen Signaturen enthält und die verschiedenen Größen, von denen jede einen Benutzer betrifft. Der Benutzer gibt selbst seine eigene Größe DH ein und es erfolgt eine Echtzeit-Berechnung durch den Leser/Codierer LE.

Die erzeugten Signaturen können unterschiedlich sein, da die gewählten Erzeugungsschlüssel verschieden sind. Dieser Unterschied kann durch eine vorher festgelegte Größe Z eingeführt werden, die ermöglicht, Benutzungszonen - entweder geographische

21.01.99

oder logische - zu unterscheiden. Es handelt sich um eine logischen Zone, wenn es darum geht, in einem Informatiksystem den Zugriff auf gewisse Programme freizugeben und auf andere nicht.

Erfindungsgemäß sind die Gebäude oder die einer Zugangskontrolle unterliegenden Systeme außerdem mit einer Prüfeinrichtung des Typs elektronische Verriegelung ausgerüstet, die in der speziellen, beschriebenen Anwendung gebildet wird durch einen Leser des Typs Kartenleser für Karten mit bündig eingelassenen Kontakten, wie in Figur 2 dargestellt, oder einen kontaktlosen Leser oder einen Magnetstreifenleser, je nach verwendetem Träger.

Dieser Leser L enthält auf klassische Weise eine Verarbeitungseinheit 200, gebildet durch einen Mikroprozessor und Speicher, die ihm zugeordnet sind: einen nichtflüchtigen Speicher 201 und einen Arbeitsspeicher 202. Der Leser umfaßt außerdem einen interne Uhr 203. In dem nichtflüchtigen Speicher (z.B. des Typs ROM) befindet sich einprogrammiert die verwendete Signaturprüfungs-funktion f sowie der Schlüssel K zum Prüfen der Signaturen.

Der Speicherungsträger umfaßt einen nichtflüchtigen Speicher 301, wobei man vorzugsweise einen elektrisch wiederprogrammierbaren Speicher wählt (NV-RAM oder EEPROM). Nach bestimmten Anwendungen kann der Speicherungsträger außerdem eine Verarbeitungseinheit des Typs Mikroprozessor 300 mit einem zugeordneten Speicher 302 des Typs ROM umfassen, die eine oder mehrere Verschlüsselungsfunktionen umfaßt. Ein solcher Speicherungsträger ist in Figur 3 schematisiert.

Die Erfindung kann vorteilhafterweise durch Briefträger für den Zutritt zu Gebäuden benutzt werden (und eventuell für die Briefkästen).

Jeder Briefträger verfügt dann über einen elektronischen Schlüssel, der ihm innerhalb eines bestimmten Zeitbereichs den Zutritt zu allen Gebäuden (und eventuell den Briefkästen dieser Häuser) einer bestimmten Zone ermöglicht. Dazu wird täglich in den Schlüssel eine gewisse Anzahl charakteristischer Informationen bzw. Daten dieser Zone und dieses Bereichs eingeschrieben.

Selbstverständlich kann die Erfindung durch jede andere Organisation benutzt werden, die häufig Zutritt zu Gebäuden haben muß. Bei dieser Anwendung sind alle in den elektronischen

21.01.99

Verriegelungen enthaltenen, zu einer bestimmten Zone gehörenden und eine bestimmte Organisation betreffenden Daten bzw. Größen identisch und der im Besitz eines Mitglieds dieser Organisation befindliche elektronische Schlüssel dient als elektronischer Passepartout.

Dem Briefträger würde es nichts nützen, den elektronischen Schlüssel zu duplizieren, da dieser nach Ablauf der Benutzungsdauer aufhört, den Zugang zu ermöglichen.

Falls die Anzahl der Benutzungen innerhalb der betreffenden Periode begrenzt ist, liefert ihm jede in seine Karte geladene Signatur Sj ein Zugangsrecht und kann nicht wiederbenutzt werden. Dazu kann die Berechnung der Signatur vorher festgelegte Parameter aj umfassen, die z.B. für alle Karten gleich sein können. Diese Parameter sind in den Verriegelungen gespeichert.

21.01.99

95 925 045.7
LA POSTE

PATENTANSPRÜCHE

1. Zugangskontrollsystem, umfassend:

- tragbare Speicherträger (C),
- Einrichtungen (LE), befähigt wenigstens einen elektronischen Schlüssel zu liefern und ihn in den im Besitz eines Benutzers befindlichen Speicherträger einzuschreiben, um ihm eine Zugangsberechtigung zu den Systemen zu geben, die man zu schützen versucht, wobei dieser Schlüssel wenigstens eine Größe DH umfaßt, die einer festgelegten Zugangsberechtigungsperiode entspricht,
- Einrichtungen (L), eine elektronische Verriegelungsfunktion sicherstellend, befähigt ein Zugangsberechtigungssignal (A) zu liefern,

dadurch gekennzeichnet, daß der gelieferte Schlüssel ebenfalls eine Signatur S der Größe DH umfaßt, wobei die zum Liefern dieses Schlüssels befähigten Einrichtungen fähig sind, auf Anfrage des Benutzers für jede neue Benutzungsperiode eine neue Signatur S zu erstellen und sie in seinen Speicherträger zu laden, um ihm seine Zugangsberechtigung so oft wie nötig zu erneuern;
und dadurch gekennzeichnet, daß die die Verriegelungsfunktion sicherstellenden Einrichtungen das Zugangsberechtigungssignal in dem Fall liefern, wo der Speicherträger (C) die Größe DH und die für die betreffende Benutzungsperiode erforderliche Signatur S im Speicher enthält, wobei diese Einrichtungen fähig sind, die Größe DH mit der betreffenden Periode zu vergleichen und zu überprüfen, ob die Signatur S tatsächlich die Signatur dieser Größe DH ist.

2. Zugangskontrollsystem nach Anspruch 1, dadurch gekennzeichnet, daß die eine festgelegte Gültigkeitsperiode betreffende Größe DH eine Benutzungsdatumsinformation und einen Benutzungsstundenbereich umfaßt.

3. Zugangskontrollsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die die Verriegelungsfunktion sicherstellenden Einrichtungen (L) einen internen Taktgeber (203) umfassen, um die gespeicherte Größe DH mit der durch den Taktgeber gelieferten Echzeit-Zeitgröße H vergleichen zu können.

21.01.99

4. Zugangskontrollsystem nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die zum Liefern wenigstens eines Schlüssels (LE) befähigten Einrichtungen eine Verarbeitungseinrichtung (100) umfassen, verbunden mit wenigstens einem nichtflüchtigen Speicher (101), in dem die Größe DH abgespeichert ist und ein Größensignaturalgorithmus f, so daß S = f (K, DH), wobei K ein Geheimschlüssel ist und der Algorithmus f ein Geheimschlüssel- oder Öffentlicher-Schlüssel-Algorithmus ist.

5. Zugangskontrollsystem nach Anspruch 4, dadurch gekennzeichnet, daß der zum Erstellen der Signaturen für alle Träger (C) benutzte Geheimschlüssel K für alle in diesen Trägern (C) geladenen und erneuerten Signaturen derselbe ist.

6. Zugangskontrollsystem nach einem der Ansprüche 4 oder 5, dadurch gekennzeichnet, daß man, um verschiedene geographische oder logische Benutzungszonen zu unterscheiden, dem zur Berechnung der Signatur S einer Größe DH benutzten Geheimschlüssel K eine je nach Zone unterschiedliche Größe Z zuordnet.

7. Zugangskontrollsystem nach Anspruch 4, dadurch gekennzeichnet, daß man verschiedene Geheimschlüssel K benutzt. um die Signaturen zu erstellen, wobei pro festgelegter geographischer oder logischer Zone ein Geheimschlüssel gewählt wird

8. Zugangskontrollsystem nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß der benutzte Geheimschlüssel ein K_C = Div (K, C) diversifizierter Schlüssel ist, wobei C eine festgelegte Größe und Div eine Diversifikationsfunktion ist.

9. Zugangskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß der festgelegte Benutzungsstundenbereich DH durch mehrere aufeinanderfolgende Stundenbereiche DHi gebildet wird, und dadurch, daß die die elektronischen Schlüssel liefernden Einrichtungen für jeden dieser Bereiche eine Signatur Si erstellen.

10. Zugangskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß mehrere Signaturen Sj berechnet und durch die zur Lieferung elektronischer Schlüssel befähigten Einrichtungen (LE) in den Trägern der Benutzer abgespeichert werden, wobei man für dieselbe Größe DH diese Signaturen aufgrund eines Geheimschlüssels K und einer Erzeugungsfunktion f erhält, z.B. Sj = f (K, DH, aj), wobei aj

21.01.99

festgelegte und in den elektronischen Verriegelungen abgespeicherte Parameter sind.

11. Zugangskontrollsystem nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die die elektronische Verriegelungsfunktion (L) sicherstellenden Einrichtungen eine Verarbeitungseinheit (200) umfassen und wenigstens einen nichtflüchtigen Speicher (201), in dem ein Signaturüberprüfungsalgorithmus und ein Signaturüberprüfungsschlüssel abgespeichert sind.

12. Zugangskontrollsystem nach Anspruch 11, dadurch gekennzeichnet, daß die die elektronische Verriegelungsfunktion (L) sicherstellenden Einrichtungen an das Lesen der Speicherträger (C) angepaßt sind.

13. Zugangskontrollsystem nach Anspruch 12, dadurch gekennzeichnet, daß die die elektronische Verriegelungsfunktion (L) sicherstellenden Einrichtungen gebildet werden durch einen Leser für Speicherkarten oder elektronische Schlüssel.

14. Zugangskontrollsystem nach Anspruch 13, dadurch gekennzeichnet, daß der Leser ein Leser für Magnetkarten ist oder ein Leser für Chipkarten mit bündig eingelassenem Kontakt oder für Chipkarten ohne Kontakt.

15. Zugangskontrollsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Speicherträger (C) einen wiederprogrammierbaren nichtflüchtigen Speicher umfassen (geschütztes bzw. gesichertes RAM, EEPROM)

16. Zugangskontrollsystem nach Anspruch 15, dadurch gekennzeichnet, daß die Träger (C) gebildet werden durch Speicherkarten mit bündig eingelassenem Kontakt oder durch Speicherkarten mit kontaktfreier Lektüre oder durch elektronische Schlüssel oder durch Magnetkarten.

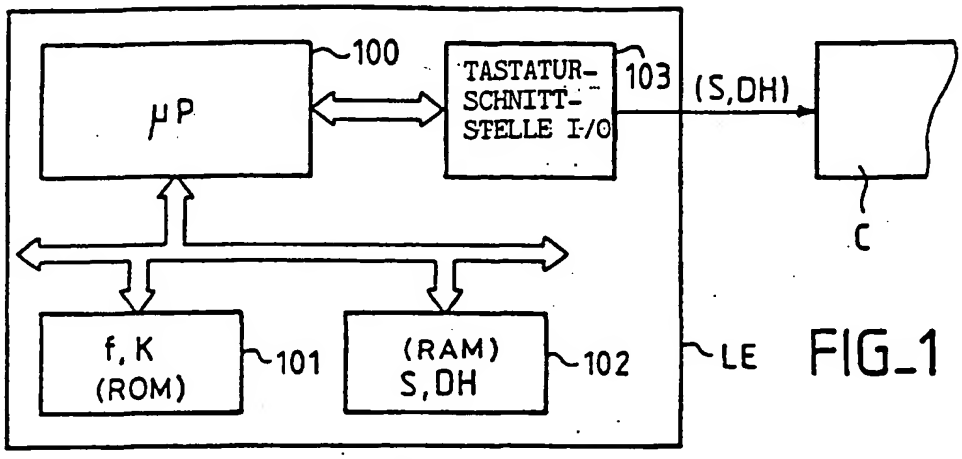
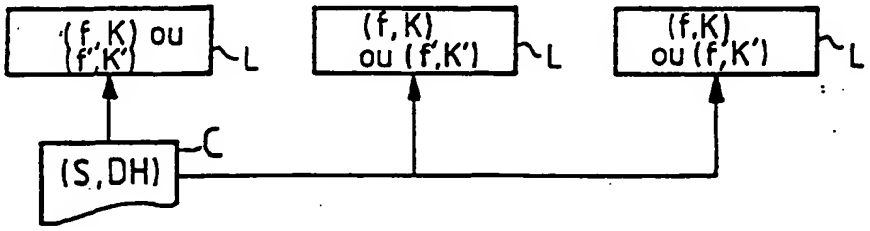


FIG_1



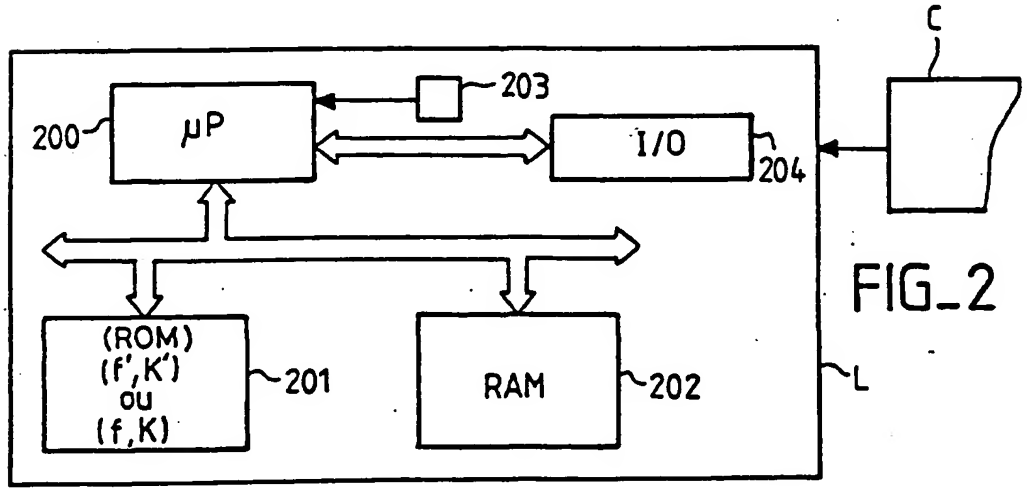


FIG_2

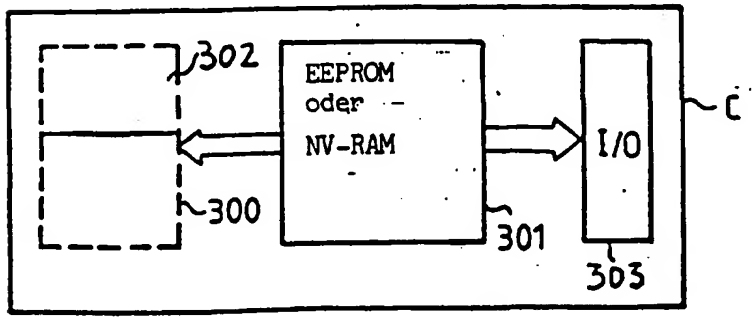


FIG_3